UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	
v.	*	**Crim. No. RDB-19-337**
DARYL ALBERT VARNUM	*	

* * * * * * * * * * *

MOTION TO SUPPRESS EVIDENCE SEIZED PURSUANT TO SEARCH WARRANTS

Defendant Daryl Varnum, through undersigned counsel, hereby moves this Honorable Court to suppress evidence seized pursuant to a search warrant dated July 5, 2019, as well as all derivative evidence, including evidence seized pursuant to subsequent search warrants, on the ground that those warrants failed to establish probable cause. Mr. Varnum also moves to suppress evidence seized pursuant to a July 24, 2019 warrant for historical cell site data. In further support, Mr. Varnum states:

I. ALLEGED FACTS

On July 5, 2019, U.S. Capital Police Special Agent Sean Wilson submitted an affidavit seeking a warrant to search (1) the person of Albert Varnum; (2) Mr. Varnum's home; (3) Mr. Varnum's 2006 Red pickup truck ("the red truck"); and (4) an apple iPhone 6 with IMEI 3S32620796E97932 ("the iPhone"). See Application for Search Warrant ("Application"), to be provided under seal in advance of hearing. Agent Wilson asserted he had probable cause to believe the warrants would produce evidence of violations of l8 U.S.C. § 115(a)(l)(A)(Threatening An Official) and l8 U.S.C. § 875(c) (Interstate Threat). Id. at 2.

The factual recitation included in the affidavit details a June 26, 2019 voicemail left at the Florida district office of a Congressperson by a person "believed to be [Mr.] Varnum." Id. at 3. The voicemail is quoted verbatim, and employs explicit language including a claim

that the caller would "come down and . . . kill" the Congressperson. Id. Agent Wilson noted that the voicemail was left by a number associated with AT&T. Id. Pursuant to an "emergency disclosure request 18 U.S.C. § 2702(c)(4)," AT&T provided Agent Wilson with subscriber information confirming that the phone number belonged to Mr. Varnum. AT&T also provided Mr. Varnum's home address. Id. These records also noted that the iPhone was registered to Mr. Varnum's account. Id. "Location information, also provided by AT&T as a result of the emergency disclosure request, showed that on June 29 and June 30, 2019, [Mr. Varnum's] cell phone was in the proximity of [Mr. Varnum's home address]." Id.[1]

The affidavit includes a summary of records provided by the "Maryland Analysis and Coordination Center" ("MCAC")[2] included detailed information about Mr. Varnum's workplace and confirming that the red truck was registered to Mr. Varnum. Id. at 3-4. The affidavit included information provided by "law enforcement agents in the U.S. Department of Defense Criminal Investigative Service" confirming that Mr. Varnum "is working at" a secure government building that prohibits the possession of cell phones or firearms while he works in the building. Id. at 4.

The affidavit closes with recitation of the alleged facts of a 2015 police report noting that Mr. Varnum's wife stated that he owned "numerous firearms," and a summary of a report

---

[1] Records received in discovery reflect that a request for this data was "initiated" by AT&T on June 30, 2019. AT&T apparently provided the location data for the phone for various times from June 29th through July 1, 2019.

[2] "The primary function of the MCAC is to provide analytical support for all federal, state and local agencies involved in law enforcement, public health and welfare, public safety and homeland security in Maryland." See http://www.mcac.maryland.gov/about_mcac/our_mission/

from the Maryland State Police noting that Mr. Varum has one handgun registered to him but does not possess a concealed carry permit. Id. at 5. The affidavit also includes reference to a Facebook posting on an account identified as belonging to Mr. Varnum. Id. In it, the author denounces a bill sponsored by the Congressperson. Id. The posting was made twelve (12) minutes after the voicemail. Id.

Based on the affidavit, the warrant was signed on July 5, 2019 and executed on July 8, 2019. That same day, Mr. Varnum was arrested and made his initial appearance on a complaint, also filed on July 5, 2019. He was indicted on July 17, 2019 and has entered a plea of not guilty.

On July 24, 2019, Agent Wilson sought a second search warrant for cell phone records associated with Mr. Varnum's telephone number. The affidavit in support of that warrant detailed Mr. Varnum's arrest, post-arrest statements made to law enforcement, and an extraction report done on the iPhone on July 23, 2019. That warrant issued and was executed on or about July 26, 2019.[3]

II. ARGUMENT

A. The Affidavit Failed to Articulate a Crime.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...." U.S. Const. Amend. IV. "As a general rule, the Fourth Amendment requires that law enforcement searches be accompanied by a warrant based on probable cause." United States v. Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018). A warrant is supported by

[3] Discovery also includes correspondence from AT&T to Agent Wilson referencing a request for information received on July 17, 2019. It is unclear exactly what information, if any, was provided pursuant to this request.

probable cause if the facts alleged in the affidavit establish "a fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Lyles, 910 F.3d 787, 791 (4th Cir. 2018). "Probable cause only exists when an officer has a reasonable belief that a law has been broken," and an "officer cannot have a reasonable belief that a violation of the law occurred when the acts to which an officer points as supporting probable cause are not prohibited by law." United States v. Williams, 740 F.3d 308, 312 (4th Cir. 2014); see also Doe v. Broderick, 225 F.3d 440, 452 (4th Cir. 2000) ("[A] mere hunch that illegal activity is afoot will not provide a valid foundation for the issuance of a search warrant.").

As a threshold matter, the affidavit failed to detail "fair probability" that Mr. Varnum committed a crime, or that his home, truck, phone, or person would yield evidence of an alleged crime. The application alleges that Mr. Varnum left a threatening voicemail, and espoused a political viewpoint in a social media posting. Political views alone cannot form the basis of the government's intrusion into sanctity of the home. See Ostergren v. Cuccinelli, 615 F.3d 263, 270-71 (4th Cir. 2010) ("The First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content."). Thus, the only criminal accusation memorialized in the application is that – over a week before the application was made - Mr. Varnum left a message threatening to kill a member of congress if that Congressperson "[did] that bill." Affidavit, 2. This, in connection with other evidence known to the government at the time of the request, is fails to provide probable cause for crime.

The Supreme Court has concluded that, in order to qualify as constitutionally unprotected criminal speech, a threatening statement must amount to a "true threat" rather

than mere political hyperbole or idle chatter. See Watts v. United States, 394 U.S. 705, 708 (1969) (per curiam). The Fourth Circuit has similarly read such a requirement into 18 U.S.C. § 115. See United States v. Roberts, 915 F.2d 889, 890–91 (4th Cir.1990).

The Fourth Circuit has identified four factors, first applied in Watts, to be relevant to determining whether a statement was a true threat: 1) whether the statement was made in jest; 2) whether it was made to a public audience; 3) whether it was made in political opposition: 4) and whether it was conditioned upon an event the speaker himself vowed would never happen. See United States v. Lockhart, 382 F.3d 447, 451–52 (4th Cir.2004). Here, the threat articulated in the search warrant affidavit was conditioned upon the Congressperson "do[ing] that bill," a vague description of an event that hadn't occurred and was overtly political. Moreover, the voicemail was left on an office voicemail service, and the political message posted to a publicly available website. Thus, both were available to an audience, one unquestionably public. Further, the application does not allege Mr. Varnum had planned for the acts alleged or taken any steps to complete them. While the voicemail does note a specific target of the threat, it doesn't connote a specific location or time for the crime to occur. It is also critical that some nine (9) days had passed without incident since the threat. Further, the affiant appears to concede that there was no effort on the part of Mr. Varnum to leave his home and travel to Florida, the location of the office where the voicemail was left, and the location of the alleged target of the threat. Against this backdrop, the voicemail appears to be crude political speech, but not a crime. Though it is true that any threat to kill is unquestionably a serious matter warranting additional investigation, the application failed to articulate an imminent "true threat" and the warrant shouldn't have issued.

Further, facts noted in the application were stale. "[T]here is no question that time is a crucial element of probable cause." United States v. Richardson, 607 F.3d 357, 370 (4th Cir. 2010). Thus, a "search warrant may issue only upon allegations of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause *at that time*." United States v. Doyle, 650 F.3d 460, 474 (4th Cir. 2011) (emphasis in original). Here, the application notes a specific alleged threat, tied to a specific legislative act (i.e., "do[ing] that bill"). There is no claim that the threat was ongoing. In fact, that well over a week had passed without incident (or even movement on the part of Mr. Varnum, who was shown by records received by AT&T to still be at or near his Maryland home and not on his way to Florida), belied the claim that the threat was imminent.

Finally, the application failed to tie the alleged crime to the locations to be searched. An "affidavit should establish a connection between the defendant and the residence to be searched and a link between the residence and any criminal activity." United States v. Martin, 297 F.3d 1308, 1314 (11th Cir. 2002). A connection between the targeted residence and the alleged perpetrator of a crime command is inherent in Lalor's command that "the crucial element is not whether the target of the search is suspected of a crime, but whether it is reasonable to believe that the items to be seized will be found in the place to be searched." United States v. Lalor, 996 F.2d 1578, 1582 (4th Cir. 1993). Indeed, "residential searches have been upheld *only* where some information links the criminal activity to the *defendant's* residence." Id. at 1583 (emphasis added). Though there is no rigid rule as to the quantum of such proof required, there must be some "firm evidence" connecting the alleged perpetrator to the home to be searched before a warrant should issue. See United States v. Kennedy, No. CIV. 07-CR-131, 2007 WL 2156611, at *5 (E.D. Va. July 25, 2007), aff'd, 292 F. App'x 240

(4th Cir. 2008) ("The warrant in this case was based on firm evidence that, prior to the incident, Michael Kennedy resided at the address to be searched . . . .").

Here, the affiant only tied alleged threats to the phone number associated with Mr. Varnum's phone, not his home or vehicle. Though information provided by AT&T tied that phone to the proximity of Mr. Varnum's home. That information was unlawfully obtained. See, infra, II (c). The warrant should not have issued.

B. The Warrant Was Overbroad.

"At its core, the Fourth Amendment protects against general warrants that authorize 'exploratory rummaging in a person's belongings . . . by requiring a particular description of the things to be seized.'" United States v. Williams, 592 F.3d 511, 519 (4th Cir. 2010) (citing Anderson v. Maryland, 427 U.S. 463, 480 (1976) (internal quotation marks omitted)). In order to ensure that the invasion of a suspect's privacy and property under a warrant is no greater than absolutely necessary, "a search is confined in scope to particularly described evidence relating to a specific crime for which there is probable cause." United States v. Oloyede, 982 F.2d 133, 138 (4th Cir. 1992) (emphasis added); see also Williams, 592 F.3d at 519 ("The particularity requirement is fulfilled when the warrant identifies the items to be seized by their relation to designated crimes and when the description of the items leaves nothing to the discretion of the officer executing the warrant.") (citations omitted).

The particularity requirement "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." Maryland v. Garrison, 480 U.S. 79, 84 (1987). "A failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a

suspect's privacy and property are no more than absolutely necessary." United States v. George, 975 F.2d 72, 76 (2d Cir. 1992). **"**The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important." United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009).

Here, the warrant sought permission to seize and search "records that might be found on [at the home, in the red truck, or on Mr. Varnum's] person, in whatever form they are found." Affidavit, 9. "One form in which the records might be found," the affiant continued, "is data stored on a computer's hard drive or other storage media such as hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media." Id. Thus, the warrant permitted a general rummaging of all electronic items for "records," leaving it to the complete discretion of the searching officers to determine what should be viewed and seized. The danger of such an expansive search was detailed in Riley:

> In 1926, Learned Hand observed . . . that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." United States v. Kirschenblatt, 16 F.2d 202, 203 (C.A.2). If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

Riley v. California, 134 S. Ct. 2473, 2490-91 (2014). The warrant was overbroad and should not have issued.

C. The Warrant Application Relied on Illegally Secured Evidence.

Under the Electronic Communications Privacy Act ("ECPA") law enforcement only may require disclosure of subscriber information under limited circumstances, including

when there is (1) a warrant, (2) a court order, (3) consent of the subscriber, or (4) an administrative subpoena. See 18 U.S.C. § 2703(c). The ECPA also authorizes companies storing electronic communications to disclose such information "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." 18 U.S.C. § 2702(c)(4). It is under this provision that authorities in this case learned most of the relevant information included in the application including the identity of Mr. Varnum, his phone number, address, and, using cell site location data, Mr. Varnum's "proximity" to that address around the time of the alleged offenses. Affidavit, 2.

Law enforcement is required to secure a warrant before receiving cell site location data. See Carpenter v. United States, 138 S. Ct. 2206, 2221, 201 L. Ed. 2d 507 (2018). Here, authorities did not secure a warrant before requesting, and receiving, that critical data from AT&T. Moreover, the law was well-established at the time of the request, leaving no excuse for police to fail to secure a warrant. Since that illegally-obtained information was critical to the issuance of the challenged warrant, suppression of the fruits of the challenged warrant must be granted. Wong Sun v. United States, 371 U.S. 471, 487–88 (1963); see also United States v. DeQuasie, 373 F.3d 509, 519 (4th Cir. 2004) (noting that the exclusionary rule "reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality or fruit of the poisonous tree.").

It bears noting that authorities ultimately did secure a warrant for cell site location data, but on July 24, 2019, well after it had apparently already received that data from Mr. Varnum's cellphone provider pursuant to its earlier, warrantless demand. Further, that

second warrant rested on illegally obtained evidence from Mr. Varnum's arrest and the July 8, 2019 search. This warrant rested on tainted evidence, and thus its fruits must be suppressed.

III. CONCLUSION

For the reasons set forth above, any response, and those arguments to be offered at a hearing on the motion, Mr. Varnum requests that this Court suppress all tangible and derivative evidence obtained as a result of the execution of the challenged warrants, and for such other relief as this Court deems just and necessary.

Respectfully submitted,

JAMES WYDA
Federal Public Defender

/s/
BRENDAN A. HURSON (#28179)
Assistant Federal Public Defender
100 South Charles Street
Tower II, 9th Floor
Baltimore, Maryland 21201
Phone: (410) 962-3962
Fax: (410) 962-0872
Email: Brendan_Hurson@fd.org

REQUEST FOR HEARING

Pursuant to Rule 105.6 of the Local Rules of the United States District Court for the District of Maryland, a hearing is requested on Defendant's motion.

/s/
BRENDAN A. HURSON
Assistant Federal Public Defender